LE PIRATAGE DE COMPTE

Définition

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne.

En pratique, les attaquants ont pu avoir accès à votre compte de plusieurs manières : le mot de passe était peut-être trop simple, vous avez précédemment été victime d'hameçonnage (phishing en anglais) où vous avez communiqué votre mot de passe sans le savoir, ou bien vous avez utilisé le même sur plusieurs sites dont l'un a été piraté.

But recherché

Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.).

Mesures Préventives

- Utilisez des mots de passes différents et complexes pour chaque site et application utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.

- Lorsque le site ou le service le permettent, **activez la double authentification** pour augmenter le niveau de sécurité.

- Ne communiquez jamais d'informations sensibles (mots de passe) par messagerie, par téléphone ou sur Internet.

- Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

- Maintenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

- N'ouvrez pas les courriels ou leurs pièces jointes et ne cliquez jamais sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont le contenu du message est inhabituel ou vide.

- Évitez les sites non sûrs ou illicites, tels ceux hébergeant des contrefaçons dont ces dernières peuvent contenir des logiciels malveillants (musique, films, logiciels, etc.) ou certains sites pornographiques.

- Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

- Si le site le permet, **vérifiez les date et heure de la dernière connexion à votre compte** afin de repérer d'éventuelles connexions anormales.

- Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics. Non maîtrisés, ils peuvent être contrôlés par un pirate.

- Déconnectez-vous systématiquement de votre compte après utilisation pour éviter que quelqu'un puisse y accéder après vous.

Si vous êtes victimes

- Si vous ne pouvez plus vous connecter à votre compte, **CONTACTEZ LE SERVICE CONCERNÉ POUR SIGNALER VOTRE PIRATAGE ET DEMANDEZ LA RÉINITIALISATION DE VOTRE MOT DE PASSE.**

- Dans vos paramètres de récupération de compte, **ASSUREZ VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS**. Si ce n'est pas le cas, changez-les immédiatement.

- CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE et choisissez en un solide (voir notre fiche sur la gestion des mots de passe). Et si possible, **ACTIVEZ LA DOUBLE AUTHENTIFICATION**.

- CHANGEZ SANS TARDER LE MOT DE PASSE PIRATÉ SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.

- PRÉVENEZ TOUS VOS CONTACTS DE CE PIRATAGE pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

- VÉRIFIEZ QU'AUCUNE PUBLICATION OU COMMANDE N'A ÉTÉ RÉALISÉE avec le compte piraté.

- Si vos coordonnées bancaires étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

- En fonction du préjudice subi, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

Les infractions encourues

• **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal)** : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.

Dans le cas d'un piratage d'un compte de messagerie :

• **Atteinte au secret des correspondances (article 226-15 du code pénal)** : délit passible d'une peine d'emprisonnement d'un an et de 45 000 euros d'amende. Dans le cas de collecte de données à caractère personnel quel que soit le compte :

• **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal)** : le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. Si le compte a été détourné pour usurper votre identité :

• **Usurpation d'identité par voie de télécommunication (article 226-4-1 du code pénal)** : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.